## REMARKS

Claims 1-26 remain in the present application. Applicants respectfully request further examination and reconsideration of the rejections based on the arguments set forth below.

### Claim Rejections – 35 U.S.C. § 103

### Claims 1-3, 5-7, 9-11, 14-15, 18-21, and 25

Claims 1-3, 5-7, 9-11, 14-15, 18-21, and 25 are rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over United States Patent Number 5,563,950 to Easter et al. (referred to herein as "Easter") in view of United States Patent Number 7,062,769 to Ma et al. (referred to herein as "Ma"). Applicants respectfully submit that the embodiments of the present invention as recited in Claims 1-3, 5-7, 9-11, 14-15, 18-21, and 25 are not rendered obvious by Easter in view of Ma for the following reasons.

Applicants respectfully direct the Examiner to independent Claim 1 that recites a processor with secure cryptographic capabilities comprising (emphasis added):

> a digital secret including a secret key used in a key-based cryptographic process, wherein the digital secret is stored only within the processor, and wherein the digital secret is operable to be used exclusively by the processor for both encryption and decryption;
>
> a cryptography engine for performing the key-based cryptographic process internally within the processor, wherein the cryptography engine is configured to access the digital secret; and
>
> internal memory coupled to the cryptography engine and configured to support the key-based cryptographic process, wherein the internal memory is further configured to store data associated with the key-based cryptographic process, wherein the data includes at least one result of a

calculation performed by the key-based cryptographic process, and wherein the data is accessible only within the processor.

Independent Claims 10 and 21 recite elements similar to independent Claim 1. Claims 2-3, 5-7, 9, 11, 14-15, 18-20, and 25 depend from their respective independent Claims and recite further elements of the claimed invention.

Page 3 of the rejection states that Easter fails to teach or suggest "wherein said internal memory is further for storing data associated with said key-based cryptographic process." Applicants concur and respectfully submit that Easter also fails to teach or suggest the elements of "wherein the internal memory is further configured to store data associated with the key-based cryptographic process" and "wherein the data includes at least one result of a calculation performed by the key-based cryptographic process" as recited in independent Claim 1.

Applicants respectfully submit that Ma, either alone or in combination with Easter, also fails to teach or suggest the elements of "wherein the internal memory is further configured to store data associated with the key-based cryptographic process" and "wherein the data includes at least one result of a calculation performed by the key-based cryptographic process" as recited in independent Claim 1. As recited and described in the present application, an internal memory is configured to store data associated with a key-based cryptographic process. The data includes at least one result of a calculation performed by the key-based cryptographic process (see, for example, line 21 of page 12 to line 5 of page 13 of the instant specification).

In contrast to the claimed embodiments, Applicants understand Ma to teach a class processor 10 with a processor 12 and a private memory 14 (Figure 1; line 56 of col. 3 to line 41 of col. 4). However, Applicants respectfully submit that Ma fails to teach or suggest that memory 14 is *configured to store data associated with a key-based cryptographic process* as claimed. Further, Applicants respectfully submit that Ma also fails to teach or suggest an internal memory configured to store data which *includes at least one result of a calculation performed by the key-based cryptographic process* as claimed. Accordingly, Applicants reiterate that Ma, either alone or in combination with Easter, also fails to teach or suggest the elements of "wherein the internal memory is further configured to store data associated with the key-based cryptographic process" and "wherein the data includes at least one result of a calculation performed by the key-based cryptographic process" as recited in independent Claim 1.

For these reasons, Applicants respectfully submit that independent Claim 1 is not rendered obvious by Easter in view of Ma, thereby overcoming the 35 U.S.C. § 103(a) rejection of record. Since independent Claims 10 and 21 recite elements similar to those discussed above with respect to independent Claim 1, Applicants respectfully submit that independent Claims 10 and 21 also overcomes the 35 U.S.C. § 103(a) rejection of record. Since dependent Claims 2-3, 5-7, 9, 11, 14-15, 18-20, and 25 recite further elements of the invention claimed in their respective independent Claims, Applicants respectfully submit

that Claims 2-3, 5-7, 9, 11, 14-15, 18-20, and 25 are also not rendered obvious by Easter in view of Ma for at least these reasons. Therefore, Applicants respectfully submit that Claims 1-3, 5-7, 9-11, 14-15, 18-21, and 25 are allowable.

Claim 4

Claim 4 is rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Easter in view of Ma, further in view of United States Patent Number 6,598,165 to Galasso (referred to herein as "Galasso"), and further yet in view of United States Patent Application Publication Number 2004/0243823 to Moyer et al. (referred to herein as "Moyer"). Applicants respectfully submit that the embodiments of the present invention as recited in Claim 4 are not rendered obvious by Easter in view of Ma further in view of Galasso and further yet in view of Moyer for the following reasons.

Applicants respectfully submit that Galasso and/or Moyer, either alone or in combination with the cited Easter/Ma combination, fail to cure the deficiencies of Easter and Ma discussed above with respect to independent Claim 1. Specifically, Applicants respectfully submit that Galasso and/or Moyer fail to teach or suggest the elements of "wherein the internal memory is further configured to store data associated with the key-based cryptographic process" and "wherein the data includes at least one result of a calculation performed by the key-based cryptographic process" as recited in independent Claim 1. Consequently, since Claims 4 recites further elements of the invention claimed in

independent Claim 1, Applicants respectfully submit that Claim 4 is not rendered obvious by Easter in view of Ma further in view of Galasso and further yet in view of Moyer. Thus, Applicants respectfully submit that Claim 4 is allowable.

Claims 8, 13, and 22

Claims 8, 13, and 22 are rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Easter in view of Ma and further in view of United States Patent Application Publication Number 2004/0098591 to Fahrny (referred to herein as "Fahrny"). Applicants respectfully submit that the embodiments of the present invention as recited in Claims 8, 13, and 22 are not rendered obvious by Easter in view of Ma and further in view of Fahrny for the following reasons.

Applicants respectfully submit that Fahrny, either alone or in combination with the cited Easter/Ma combination, fails to cure the deficiencies of Easter and Ma discussed above with respect to independent Claims 1, 10, and 21. Specifically, Applicants respectfully submit that Fahrny fails to teach or suggest the elements of "wherein the internal memory is further configured to store data associated with the key-based cryptographic process" and "wherein the data includes at least one result of a calculation performed by the key-based cryptographic process" as recited in independent Claim 1, and similarly recited in independent Claims 10 and 21. Consequently, since Claims 8, 13, and 22 recite further element of the invention claimed in their respective independent Claims, Applicants respectfully submit that Claims 8, 13 and 22 are not rendered obvious

by Easter in view of Ma and further in view of Fahrny. Thus, Applicants respectfully submit that Claims 8, 13, and 22 are allowable.

Claim 12

Claim 12 is rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Easter in view of Ma and further in view of United States Patent Number 6,031,992 to Cmelik et al. (referred to herein as "Cmelik"). Applicants respectfully submit that the embodiments of the present invention as recited in Claim 12 are not rendered obvious by Easter in view of Ma and further in view of Cmelik for the following reasons.

Applicants respectfully submit that Cmelik, either alone or in combination with the cited Easter/Ma combination, fails to cure the deficiencies of Easter and Ma discussed above with respect to independent Claim 10. Specifically, Applicants respectfully submit that Cmelik fails to teach or suggest the elements of "wherein the internal memory is further configured to store data associated with the key-based cryptographic process" and "wherein the data includes at least one result of a calculation performed by the key-based cryptographic process" as recited in independent Claim 1, and similarly recited in independent Claim 10. Consequently, since Claim 12 recites further elements of the invention claimed in independent Claim 10, Applicants respectfully submit that Claim 12 is not rendered obvious by Easter in view of Ma and further in view of Cmelik. Thus, Applicants respectfully submit that Claim 12 is allowable.

Claims 16 and 17

Claims 16 and 17 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Easter in view of Ma and further in view of United States Patent Application Publication Number 2004/0025036 to Balard et al. (referred to herein as "Balard"). Applicants respectfully submit that the embodiments of the present invention as recited in Claims 16 and 17 are not rendered obvious by Easter in view of Ma and further in view of Balard for the following reasons.

Page 17 of the rejection suggests that the cited Easter/Ma combination fails to teach or suggest "wherein said digital secret comprises a random number that is generated from an HMAC algorithm implemented on testing data associated with fabrication of said IC chip." Applicants concur and respectfully submit that Easter and/or Ma also fail to teach or suggest the elements of "wherein the digital secret is calculated using an HMAC algorithm implemented on testing data, and wherein the testing data is associated with fabrication of the processor" as recited in Claim 16.

Applicants respectfully submit that Balard, either alone or in combination with Easter and/or Ma, also fails to teach or suggest the elements of "wherein the digital secret is calculated using an HMAC algorithm implemented on testing data, and wherein the testing data is associated with fabrication of the processor" as recited in Claim 16. In contrast to the claimed embodiments, Applicants fail to find any teaching or suggestion in Balard of a digital secret calculated using an HMAC algorithm as claimed. Additionally, Applicants fail to find any teaching or

suggestion in Balard of a digital secret calculated using an HMAC algorithm *implemented on testing data* as claimed. Applicants also fail to find any teaching or suggestion in Balard of a digital secret calculated using an HMAC algorithm implemented on testing data which is *associated with fabrication of the processor* as claimed. Accordingly, Applicants reiterate that Balard, either alone or in combination with Easter and/or Ma, also fails to teach or suggest the elements of "wherein the digital secret is calculated using an HMAC algorithm implemented on testing data, and wherein the testing data is associated with fabrication of the processor" as recited in Claim 16.

Further, Applicants respectfully submit that Balard, either alone or in combination with the cited Easter/Ma combination, fails to cure the deficiencies of Easter and Ma discussed above with respect to independent Claim 10. Specifically, Applicants respectfully submit that Balard fails to teach or suggest the elements of "wherein the internal memory is further configured to store data associated with the key-based cryptographic process" and "wherein the data includes at least one result of a calculation performed by the key-based cryptographic process" as recited in independent Claim 1, and similarly recited in independent Claim 10. Consequently, since Claims 16 and 17 recite further elements of the invention claimed in independent Claim 10, Applicants respectfully submit that Claims 16 and 17 are not rendered obvious by Easter in view of Ma and further in view of Balard. Thus, Applicants respectfully submit that Claims 16 and 17 are allowable.

Claims 23, 24, and 26

Claims 23, 24, and 26 are rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Easter in view of Ma and further in view of Moyer. Applicants respectfully submit that the embodiments of the present invention as recited in Claims 23, 24, and 26 are not rendered obvious by Easter in view of Ma and further in view of Moyer for the following reasons.

Applicants respectfully submit that Moyer, either alone or in combination with the cited Easter/Ma combination, fails to cure the deficiencies of Easter and Ma discussed above with respect to independent Claim 21. Specifically, Applicants respectfully submit that Moyer fails to teach or suggest the elements of "wherein the internal memory is further configured to store data associated with the key-based cryptographic process" and "wherein the data includes at least one result of a calculation performed by the key-based cryptographic process" as recited in independent Claim 1, and similarly recited in independent Claim 21. Consequently, since Claims 23, 24, and 26 recite further elements of the invention claimed in independent Claim 21, Applicants respectfully submit that Claims 23, 24, and 26 are not rendered obvious by Easter in view of Ma and further in view of Moyer. Thus, Applicants respectfully submit that Claims 23, 24, and 26 are allowable.

## CONCLUSION

Applicants respectfully submit that Claims 1-26 are in condition for allowance and Applicants earnestly solicit such action from the Examiner.

The Examiner is urged to contact Applicants' undersigned representative if the Examiner believes such action would expedite resolution of the present application.

Please charge any additional fees or apply any credits to our PTO deposit account number: 50-4160.

Respectfully submitted,

MURABITO, HAO & BARNES LLP

Dated: 5 / 7 / 2009 /BMF/

Bryan M. Failing
Registration No. 57,974

Two North Market Street
Third Floor
San Jose, CA 95113
(408) 938-9060